DETERMINATION OF THE CHIEF MANAGEMENT OFFICER

Under the authority delegated to me by the Secretary of Defense, I have determined that the following information is exempt from disclosure under Exemption 3 of the Freedom of Information Act (5 U.S.C. § 552(b)(3)) because it meets the requirements for exemption under 10 U.S.C. § 130e:

> Defense Information Networks architecture and engineering information.

Date: 10-19-18

For John H. Gibson II
Chief Management Officer of the
Department of Defense

STATEMENT OF THE BASIS FOR THE DETERMINATION BY THE CHIEF MANAGEMENT OFFICER

In accordance with 10 U.S.C. § 130e, I reviewed information regarding Department of Defense Information Network (DoDIN) architecture, infrastructure, design, and engineering. I have determined that this information qualifies as defense critical infrastructure security information (DCRIT). As defined by 10 U.S.C. § 130e, DCRIT includes:

> "…sensitive but unclassified information that, if disclosed, would reveal vulnerabilities in Department of Defense critical infrastructure that, if exploited, would likely result in the significant disruption, destruction, or damage of or to Department of Defense operations, property, or facilities, including information regarding the securing and safeguarding of explosives, hazardous chemicals, or pipelines, related to critical infrastructure or protected systems owned or operated by or on behalf of the Department of Defense, including vulnerability assessments prepared by or on behalf of the Department of Defense, explosives safety information (including storage and handling), and other site-specific information on or relating to installation security."

The DoDIN is the Department of Defense's (DoD) globally interconnected, end-to-end set of electronic information capabilities and associated processes for collecting, processing, storing, disseminating, and managing digital information on-demand to warfighters, policy makers, and support personnel, including owned and leased communications and computing systems and services, software (including applications), data, security services, and other associated services, and National Security Systems. The DoDIN includes a wide variety of information systems, including but not limited to the Defense Information Systems Network, the Joint Information Enterprise, DoD Component information systems and networks (to include Communities of Interest (e.g., Medical Community of Interest) and Programs of Record (e.g., High Performance Computing Modernization Program)). Because DoD operational missions depend upon a secure, streamlined information technology and cyber infrastructure, it is imperative that adversaries or potential adversaries do not gain access to information detailing the DoDIN architecture, infrastructure, design, data flows, and engineering. Gaining this information about the Department's cyber capabilities and dependencies, individually or in the aggregate, would enable an adversary to locate, identify and target critical military functions and exploit operational vulnerabilities. This information would inform adversary efforts to disrupt or incapacitate the execution of core missions, thereby introducing a serious risk to not only U.S. military operations, but also U.S. Federal Government National Security Systems as defined by National Security Directive 42.

The categories of information associated with unclassified DoDIN that qualify as DCRIT include:

- Detailed system requirements and specifications;
- Security documentation;
- Disaster recovery and continuity of operations planning;
- Analysis of the potential for exploitation and potential threat impact to the DoDIN;

- DoDIN risk assessments;

- Site and system configurations;

- Details of circuit and internal routing information;

- Circuit and routing troubleshooting and maintenance actions;

- Network depictions (drawings, topology, or graphics) when legends or other explanatory material reveals sensitive terminology or relationships;

- Fault reporting;

- Operational logs, such as master station logs, containing information on daily operations;

- Raw or summary data for traffic density and patterns;

- Circuitry performance information regarding threat or vulnerability mitigation;

- Information which reveals or describes DoDIN and National Security Systems cybersecurity capabilities or methods, to include descriptions of compliance with security controls used to combat published threats without further association;

- Detailed network Security Architecture diagrams;

- Identification of operations systems, software, and hardware configurations;

- The specific capability being pursued by the U.S. Government in response to a stated cybersecurity mission need or commercially identified cyber vulnerability;

- General test plans or test objectives; and

- Specific configuration settings of cyber sensors and other Defensive Cyber Operations devices.

I considered the public interest in the disclosure of DoDIN sensitive information and weighed this against the risk of harm that might result if this information were to be disclosed. Because the public interest in the disclosure is minimal, and the risk of harm that might result from this information is extremely significant, I have determined that the protection of this information is critical to the security of the DoD infrastructure and should be exempt from disclosure.